

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-304809
(43)Date of publication of application : 18.10.2002

(51)Int.Cl. G11B 20/10
G06F 12/14
G11B 7/004
G11B 7/26
G11B 20/12

(21)Application number : **2002-018468**
(22)Date of filing : **28.01.2002**

(71)Applicant : **EASTMAN KODAK CO**
(72)Inventor : **BARNARD JAMES A
INCHALIK MICHAEL A
HA BRUCE L**

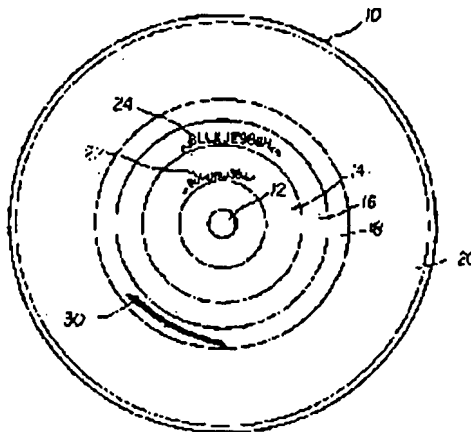
(30)Priority
Priority number : 2001 772333 Priority date : 29.01.2001 Priority country : US

(54) COPY PROTECTION USING A PREFORMED ID AND A UNIQUE ID ON A PROGRAMMABLE CD-ROM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for making copy protection that cannot be subverted by a bit-for-bit copying scheme on standard CD-writers.

SOLUTION: This invention provides a copy-protected optical disk, including a pre-formed ID, which is impressed upon the optical disk during optical disk manufacture, a unique ID which was written on the optical disk after it is manufactured, and an encrypted program written onto the optical disk wherein the encryption of such program is based upon the performed ID and the unique ID.



LEGAL STATUS

[Date of request for examination]	24.01.2005
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	withdrawal
[Date of final disposal for application]	27.04.2005

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-304809

(P2002-304809A)

(43) 公開日 平成14年10月18日 (2002. 10. 18)

(51) IntCl ⁷	識別記号	F I	テーマコード*(参考)
G 1 1 B 20/10	3 0 1	G 1 1 B 20/10	H 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 0 1 Z 5 D 0 4 4
G 1 1 B 7/004		G 1 1 B 7/004	3 2 0 F 5 D 0 9 0
7/26		7/26	Z 5 D 1 2 1
審査請求 未請求 請求項の数 3 O L (全 14 頁) 最終頁に続く			

(21) 出願番号 特願2002-18468(P2002-18468)

(22) 出願日 平成14年1月28日 (2002. 1. 28)

(31) 優先権主張番号 7 7 2 3 3 3

(32) 優先日 平成13年1月29日 (2001. 1. 29)

(33) 優先権主張国 米国 (U S)

(71) 出願人 590000846

イーストマン コダック カンパニー
 アメリカ合衆国, ニューヨーク14650, ロ
 チェスター, ステイト ストリート343

(72) 発明者 ジェイムズ エイ バーナード

アメリカ合衆国 ニューヨーク 14546
 スコッツヴィル チリ・アヴェニュー 51

(72) 発明者 マイケル エイ インチャリック

アメリカ合衆国 ニューヨーク 14534
 ビッツフォード カッパー・ウッズ 30

(74) 代理人 100070150

弁理士 伊東 忠彦

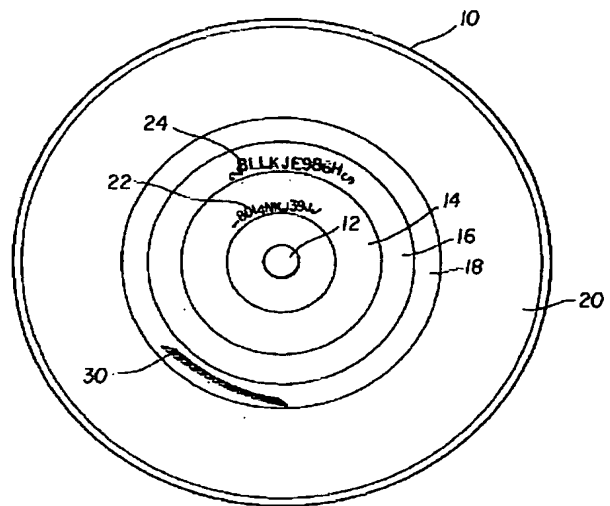
最終頁に続く

(54) 【発明の名称】 予め形成された I D および固有の I D を利用したプログラム可能な C D - R O M におけるコピ
 ー・プロテクト

(57) 【要約】

【課題】 標準的な C D ライタでビットに関するコピー
 手法によって破られないコピー・プロテクトを行う手法
 を提供すること。

【解決手段】 本発明によれば、コピー・プロテクトさ
 れた光学ディスクが提供される。光学ディスクは、光学
 ディスクの製造中に光学ディスクに記された予め形成さ
 れた I D と、製造後に前記光学ディスクに書き込まれた
 固有の I D と、光学ディスク上に書き込まれた暗号化さ
 れたプログラムとを有する。そのプログラムの暗号化
 は、前記予め形成された I D および前記固有の I D に基
 づいて行われる。



(2) 002-304809 (P2002-304809A)

【特許請求の範囲】

【請求項1】 コピー・プロテクトされた光学ディスクであって：

- a) 光学ディスクの製造中に光学ディスクに記された予め形成されたID；
 - b) 製造後に前記光学ディスクに書き込まれた固有のID；および
 - c) 前記光学ディスク上に書き込まれた暗号化されたプログラム；
- より成り、そのプログラムの暗号化は、前記予め形成されたIDおよび前記固有のIDに基づいて行われることを特徴とする光学ディスク。

【請求項2】 光学ディスクに記録された情報をコピー・プロテクトする方法であって：

- a) 予め形成されたIDを含むマスタ・ディスクを形成するステップ；
 - b) 前記マスタ・ディスクと同一の予め形成されたIDを有する複数の光学ディスクを形成するステップ；
 - c) 光学ディスクに固有の識別番号を書き込むステップ；および
 - d) 前記光学ディスクに暗号化されたプログラムを書き込むステップ；
- より成り、そのプログラムの暗号化は、前記予め形成されたIDおよび前記固有のIDに基づいて行われることを特徴とする方法。

【請求項3】 プログラム可能なCD-ROMおよび暗号化解除プログラムを利用してコピー・プロテクトを行う方法であって：

- a) プログラム可能なCD-ROMの予め形成されたIDおよび固有のIDを読み出すステップ；
 - b) 前記予め形成されたIDおよび固有のIDを結合して暗号解除キーを作成するステップ；
 - c) 前記暗号解除キーを利用して、当初の実行可能なファイルの暗号化を解除するステップ；
 - d) 当初の実行可能なものをコンピュータのRAMメモリに格納し、それを実行することを許容するステップ；
- および
- e) 前記実行可能なものの実行完了時に、前記コンピュータのメモリから前記当初の実行可能なものを削除するステップ；
- より成ることを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、コンパクト・ディスクその他の光学的に記録されたディスクに記録された情報に対するコピー・プロテクトに関する。

【0002】

【従来の技術】 オーディオ、映像、ソフトウェアまたはデータを含む光学ディスクの消費者購買層は数十億ドル市場を生み出した。近年における低価格の光学的記録媒体

およびドライバの出現は、権限なしにその内容をコピーすることを普及させた。これに対処するために、様々なコピー・プロテクト手法が開発された。しかしながらこれらの手法の内のあるものは、デジタル・データ・ストリームの特徴を利用し、これは精巧な低価格のレコードにより、ビットに関するコピー (bit-for-bit copy) を利用してコピーされ得る。他には、書き込みおよび読み込みの両者を困難にするように光学ディスクの特徴を変化させるものがある。さらには、ネットワーク接続または2次的な「キー」(key)ディスク手法を使用し、独立した(スタンドアロンの)プロテクトを許容しないものもある。

【0003】 Horstmann (U.S. 6,044,469) は、プロテクタ・モジュールを利用したソフトウェア保護機構を開示し、これはライセンス・ファイルを読み出し、購入したそのライセンスに基づく規則を実行する。これは論理レベルにおけるソフトウェアを保護し、特に、権利が認められていないソフトウェアの部分に対する保護である。このシステムがコンパクト・ディスクに包含されるならば、標準的なCDライタを利用したそのディスクの再生成は、総ての既存のアクセスに関するコピーを正当なものにするであろう。

【0004】 Asai et al (U.S. Re. 35,839) は、データを格納するコンパクト・ディスクにおける識別領域を利用する方法を開示し、これはディスクの他の場所に格納されたデータと比較され、真正であることを確認する。これは論理レベルにおけるデータを保護するが、そのディスクに関する単純なビットに関するコピーによって、そのプロテクトは破られてしまう。

【0005】 DeMont (U.S. 5,982,889) は、情報製品 (information product) に対するユーザ・アクセスが真正であることを確認する方法を教示する。このシステムの欠点は、その真正確認が中央局を介して行われることである。ネットワークに接続することを希望しない(または不可能な)ユーザは、この製品を利用することができない。

【0006】 Hasebe, et al (U.S. 5,555,304) は、ユーザ各自または使用されるコンピュータに関連するシステムを開示する。これは、単独のコンピュータにおけるプログラムの利用を真正のユーザに限定し、ユーザの移動性またはそれらの設備のアップ・グレードを非常に制限する。さらに、この特許は、ディスクの再書き込み不可能な領域に格納されたデータの利用にも関連し、再書き込み不可能なリーフ (leaves) が形成されるその手法は、(「再書き込み不可能な」部分も含めて) データを新たなディスクにコピーする機能を開放する。

【0007】 Fite et al による一連の特許 (U.S. 5,400,319, 5,513,169, 5,541,904, 5,805,549, および 5,930,215) は、規定可能なコードを生成するようにディスクの小領域から反射層を選択的に除去することによって、光

(3) 002-304809 (P2002-304809A)

学ディスクに機械的に読み取り可能なシリアル番号コードを形成する方法を開示する。このようなシステムに対する欠点は、この特殊なコードを書き込むために特殊な装置が必要とされることである。

【0008】Kanamaru (U.S. 5,940,505) は、どのようにしてCD-ROMがコピー・プロテクトされるかを教示する。しかしながら、Kanamaru の発明の総ての装置は、ディスク上の情報を解読するために、組み込み回路形式でまたは付加的なコンピュータ・ボード形式で、補助的なハードウェアを要する。

【0009】O' Connor et al. による米国特許第5,745,568号は、特定のコンピュータ・システムによって回復されるCD-ROMデータを保全する方法およびシステムを開示する。光学ディスクの領域は、暗号キーとしてのハードウェア識別子を用いて暗号化される。ハードウェア識別子は、選択されたコンピュータ・ハードウェアに関連する。CD-ROMに含まれるソフトウェア・プログラム・ファイルは、暗号キーとしてのハードウェア識別子を利用して暗号化される。CD-ROM上の選択されたソフトウェア・プログラムは、暗号キーとしてのハードウェア識別子を利用するソフトウェア・プログラム・ファイルを解読することによって、その選択されたコンピュータ上でインストールされる。

【0010】Akiyama et al. による米国特許第5,805,699号は、マスタ記憶媒体に記録された著作物ソフトウェアを、合法的な手法で、ユーザのターゲット記憶媒体にコピーさせることを可能にするソフトウェア・コピー・システムを提案する。マスタ記憶媒体（すなわち、CD-ROM）は、ソフトウェア識別子を有し、ターゲット記憶媒体は記憶媒体識別子を有する。これら2つの識別子が中央局に伝送され、中央局はソフトウェア製品をコピーするための権利に関するライセンス（契約）を管理している。中央局において、2つの識別子から第1の署名が生成され、コンピュータ・ユーザに返送される。ユーザのコンピュータにおいて、その2つの識別子から第2の署名が生成される。2つの署名が互いに一致する場合に限って、マスタ記憶媒体からターゲット記憶媒体へソフトウェア・プログラムがコピーされ得る。

【0011】Chandra et al. による米国特許第4,644,493号は、単独のコンピュータで使用する磁気媒体で利用されるソフトウェアの配布を制限する方法および装置を開示する。磁気媒体に含まれる当初のソフトウェアは、機械的にコピー不可能である。これは、コンピュータの一部をなす不正操作のきかないコプロセッサに格納されたプログラムを実行することによってそれが修正されるまでその状態が続く。

【0012】Indeck et al. による米国特許第5,740,244号は、磁気媒体上のソフトウェア製品が最初にコンピュータに命令することによる改善を開示し、その磁気媒体を挿入すると、その製品の特定の部分の指紋を読み取

り、その指紋とその同じ指紋に関して予め記録されていたものとを比較する。指紋が一致していれば、ソフトウェア製品は、コンピュータが更に読み込むことを許容し、そこに格納されているアプリケーション・ソフトウェアを実行可能にする。

【0013】これらの手法に関連して多くの問題が存在する。1つには、これらの多くが「ハック」(hacks)と呼ばれるものに対して無防備なことである。この意味することは、あるユーザが解読する又はそのアプリケーションを利用する方法を判別すると、その種の者にとって、そのアプリケーションへのアクセスを取得する方法を広めることは非常に容易であるということである。特定のハードウェアの組み合わせに依存した特定のアプリケーションを利用することによって、この問題を解決するものもある。その手法は携帯性に関する問題を生み出す。合法的なユーザであっても場所が異なればコンピュータ上のアプリケーションを利用できないのである。ユーザが、例えばアップ・グレードによりハードウェアの構成(configuration)を変更すると、そのアプリケーションは起動することができない。

【0014】

【発明が解決しようとする課題】従って、本発明は、標準的なCDライターでビットに関するコピー手法によって破られないコピー・プロテクトを行う手法を提供することを目的とする（ただし、これは標準的なCDマスタおよびライト設備で実行可能なものである。）。

【0015】

【課題を解決するための手段】この課題を解決するコピー・プロテクトされた光学ディスクは：

a) 光学ディスクの製造中に光学ディスクに記された予め形成されたID；

b) 製造後に前記光学ディスクに書き込まれた固有のID；および

c) 前記光学ディスク上に書き込まれた暗号化されたプログラム；

より成り、そのプログラムの暗号化は、前記予め形成されたIDおよび固有の識別番号に基づいて行われる光学ディスクである。

【0016】本発明は、一般のハッカによる発見を防止しつつ携帯性をも提供し、認証されているユーザが単独のコンピュータ・システムを利用することに関して制限されないようにする。多くの従来技術とは異なり、ソフトウェアが利用される又はインストールされるときに、接触する権限を付与する中央管理的な権利は必要としない。

【0017】物理的形態のキー（予め形成されたID）および論理的形態のキー（固有のID）の両者を利用することによって、多くの複製手法を排除する。単純なビットに関する複製(bit-for-bit duplication)が回避される。なぜなら、予め形成されたIDをコピーしないか

(4) 002-304809 (P2002-304809A)

らであり、これはディスク・トラックの物理的構造に符号化されている。複数ユーザまたは複数の顧客の間でのソフトウェアの「共有」が回避される。なぜなら、そのように共有されるソフトウェアは、(よく起こるであろう事態として)両ユーザが予め形成されたIDを利用してディスクを使用しようとする場合であっても、適切な固有のIDなしには走らないからである。その記録手法は、ロック(lock)された実行可能なファイルを形成する。

【0018】

【発明の実施の形態】図1を参照するに、本発明によるコピー・プロテクトされた光学ディスク10が示されている。これはプログラム可能なCD-ROMディスクであり、予め記録されたマスタ領域(mastered pre-recorded area)(ROM領域)および記録可能な領域(RAM領域)の両者を含む。ディスク10を回転させるための中心軸に関するホール12がある。この特定のプログラム可能なCD-ROMディスクは、マスタ化された第1セッション(session)14を有し;すなわち、マスタ・ディスクが、第1セッション14において供給されるソフトウェアまたはデータを包含して形成され、その後、直接的に又は中間的な「父」および「母」ディスクを介して、ディスク10の多くのコピーに印を付すために使用される。プログラム可能なCD-ROMをマスタ化する技術は、本願と共通して譲渡され、2000年9月15日付けで出願され、Ha et alによる“System for Making aPhotoresist Master of a Hybrid Optical Recording Disc”と題する米国特許出願番号09/662,561号に詳細に説明されており、その開示内容は本願でも使用可能である。

【0019】プログラム可能なCD-ROMを含む書き込み可能なコンパクト・ディスクは、部分的に溝変調(groove modulation)を使用する。ディスク10は、基板の内側端部から外側端部に伸びる連続的ならせん状トラックを有する。らせん状トラックは通常は溝であり、ディスク10にデータ・チャンネルを提供し、データの読み込みまたは書き込みの最中にディスク10のトラッキング(tracking)をも提供する。溝はその溝に垂直な方向の振動を有し、それゆえに揺動した溝(wobbled groove)または運動的な溝(wobble groove)としても言及される。データをアドレスおよびプログラムする配置に加えて、プログラム可能なCD-ROM光学記録ディスクのトラック又は溝、溝の変調度は、オレンジ・ブック・パート2仕様1(Orange Book Part II specification)に従って提供されるのが普通である。「オレンジ・ブック・パート2」は、フィリップス・インターナショナルBVにより公表された仕様であり、記録可能なコンパクト・ディスク媒体のキー(key)特性および記録特性を規定する。

【0020】溝の振動周波数は、プレ・グループにおける絶対時間(ATIP: Absolute Time In Pre-groove)とし

て知られる信号を利用して変調される。ATIPは、光学ディスク10の記録面全体に関するトラックの場所に関する情報を含む。オレンジ・ブック仕様によれば、ATIP信号は22.05kHzのFM信号であり、3150ビット/秒のレートでデータを搬送する。このデータは、毎秒7542ビット・フレームとして特定される。データ領域において、各フレームは、4つの同期ビットと、分カウントを表現する8ビットと、秒カウントを表現する8ビットと、フレーム・カウントを表現する8ビットより成る。分、秒およびフレーム・カウントは、2つの4ビット2進化10進数(BCD)より成る。ディスク10のデータ領域において、これらの値の任意のものについての最大値は75であり、各々の最上位ビット(MSB)は常にゼロである。そして、分カウント、秒カウントおよびフレーム・カウントの最上位ビットの3つは、全体として、000の2進値を有する。各フレームの最後の14ビットは、巡回冗長検査(CRC: cyclic redundancy check)誤り保護として提供される。

【0021】直径46mmないし50mmの間のディスク10の領域として定義されるディスク導入領域(lead-in area)において、MSBの値は000から変化する。100という値は、そのフレームが、電力校正領域(Power Calibration Area)、プログラム・メモリ領域または導入領域(Lead-In Area)に関する時間コードを含むことを意味し、これら総てはプログラム(記録可能な)領域の前に設けられる。他のMSB値は、ATIPフレームが特殊な制御コードを含むことを規定するために使用される。これらのコードは、例えば、ディスク10に関する最適な書き込み電力、参照速度、ディスク・アプリケーション・コード、ディスク形式および副形式、導入領域の開始位置またはディスク10に関する導出領域(Lead-Out Area)の開始位置を指示するために使用される。

【0022】プログラム可能なCD-ROM光学ディスクのROM領域において、溝は、データをアドレスするディスク10およびデータをプログラムするディスクに対応してくぼんだ形状で(depression)更に変調される。CD上でオーディオでない情報が格納されているフォーマットは、「イエロー・ブック」(Yellow Book)規格として知られている。

【0023】ディスク10の第1セッション14(ROM領域)は、予め形成された識別番号またはID22を含み、これはマスタ・プロセスの間に記録され、そして各プログラム可能なCD-ROMディスクに押印されたデジタル署名である。予め形成されたID22は、ATIP信号内にまたはディスク・プログラム可能なCD-ROM・データ信号内に設けることが可能である。好適実施例では、1つ又はそれ以上の特定の制御コードを利用して、導入領域におけるATIP信号に設けられる。例えば、ディスク・アプリケーション・コード、ディスク形式、ディスクに関する最適な書き込み電力、参

(5) 002-304809 (P2002-304809A)

照速度、導入領域の開始位置、導出領域の開始位置、またはオレンジ・ブックにより定められる他の特殊または付加的な情報は、ディスク製造者に既知の特殊な値に設定されることが可能である。これらの値は単独で又は組み合わせて、予め形成されたID22コードを算出するために使用可能である。

【0024】ディスク10は第2セッション16を含み、CD-WOまたはCD-RWライタのような再記録可能な光学ディスク技術を利用して書き込まれたものである。ディスク10は、第3セッションを含むことも可能であり、あるいは更に後続の書き込み済みセッション(written session)を含むことも可能である。ディスク10は、ユーザの再記録可能な領域20をも包含する。記録済みのセッションに含まれているものは、固有の識別番号またはID24および暗号化された実行可能な(executable)パッケージ30であり、ID24は1つ又はそれ以上の既知の絶対セクタ・アドレスにおける第2セッションに書き込まれる。

【0025】図2を参照するに、本発明で使用する実行可能なプログラムを暗号化する手法の1つが示されている。実行可能なパッケージはディスク10に書き込まれる。暗号化されたパッケージは6つの実行可能なプログラム30を含み、これはディスク10において当初の実行可能なプログラム40と同一名称を有する。パッケージ30は、最初に走るラッピング(wrapping)ソフトウェアを含む。このパッケージは、プログラムが走っている際に、ハッキング・ソフトウェアの存在を検査するサブルーチン34も含む。また、データ、命令または両者より成る多形態セクション36も存在する。概して多形態コードは、同一結果に導く複数の経路を提供するが、プログラムが実行される各々の場合に異なる経路をたどるように構成される。多形態コードは、そのプログラムに対するリバース・エンジニアリングを一層困難にするために使用される。暗号解除ルーチン38は、プログラム可能なCD-ROMに格納されたデータ(特に、予め形成されたID22および固有のID24)を利用するために指定され、実行可能なもの40の暗号化を解除する。

【0026】図3を参照するに、ユーザの実行可能なプログラムを暗号化するために必要なステップが示され、それを暗号化するためにプログラム可能なCD-ROMの特性を利用する。これは、本願で詳細に説明される様々な本願実施例で使用可能である。ステップ48において、プログラム可能なCD-ROM上に又は局所的なハード・ドライブ上もしくは配信ネットワーク上にマスタされた(mastered)暗号化プログラム可能なCD-ROMが、コンピュータのメモリ内に読み込まれる。ステップ50において、暗号化を要する実行可能なファイルがメモリに読み込まれる。ステップ52において、ソフトウェア・アプリケーションを拡布する者またはプログラム

可能なCD-ROMを利用する存在として定められる顧客は、マスタされたプログラム可能なCD-ROMディスクをCD-ROMライタに置く。

【0027】顧客が暗号化されるべきファイルを指定することによって開始する。これらのファイルは、データおよび実行可能なプログラムの両者または実行可能なプログラムだけを含み得る。その後顧客は、暗号化されたソフトウェアが書き込まれるべきプログラム可能なCD-ROMディスクに関する予め形成されたID22および固有のID24に対応する情報を入力する。他の実施例にあっては、これらの値は、それらが記録される任意の場所からプログラム可能なCD-ROMから読み出される。セキュリティ・ソフトウェアが予め形成されたID22および固有のID24を取得すると、ステップ62において、それらを共に利用して暗号キーを作成する。暗号化プログラム63は、ステップ64においてその暗号キーを利用し、実行可能なファイルおよびセキュリティ・レベル・テーブルを暗号化する。ステップ64で暗号化されたファイルは、その後ステップ70においてラッパ(wrapper)プログラムにデータ・ファイルとして付加される。ラッパ・プログラムは、セキュリティ・テーブルにおける指定によって許容されるようなディスク10からの予め形成されたID22および固有のID24を読み込むのに必要なサブルーチンと、プログラムが走っているコンピュータのメモリ内にリバース・エンジニアリング・ツールが存在することを検出し、それらが検出された場合には実行を中断させるサブルーチンと、ソフトウェア・アプリケーションの暗号化解除および実行を開始するサブルーチンとを含む。ステップ72において、ラップされた実行可能パッケージは、書き込み可能セッション(16または18)においてプログラム可能なCD-ROMディスクに書き込まれる。

【0028】暗号作成法および暗号化機能は当該技術分野で周知である。これに関し、Applied Cryptography, B.Schneier, John Wiley and Sons, Inc., New York, 1996に適切な記載があり、この内容は本願でも使用可能である。本実施例では、以下の表記方法を採用する：

表1

暗号化標記

記号	意味
P	暗号化されるべきプログラム
E	暗号化関数
B	予め形成されたID
U	固有のID
I	連結したID=B U
X	暗号化されたプログラム=E (P, I)

本発明に関し、以下の条件を満足する任意の暗号化関数が利用可能であり、それは： $E(P, I)$ の計算が実行可能に適切であること、すなわちEが多項式タイム(poly-nomial time)で計算可能であること； $E^{-1}(X, I)$

(6) 002-304809 (P2002-304809A)

の計算に関する多項式タイム・アルゴリズムが既知であって実行可能に適切であること；暗号化関数 E （およびその解読に相当する E^{-1} ）が、その計算の際に提供される可変なキー I を利用すること；および暗号化／暗号解除プロセスを通じて良好でないプログラム P' （ $P' = E^{-1}(E(P, I), I)$ ）を形成してしまう蓋然性が非常に小さいこと、である。

【0029】暗号化のステップは以下のとおりである：

1. 予め形成されたID Bおよび固有のID Uを取得する；
2. 2つのIDが連結され（ $I = BU$ ）、暗号化／暗号化解除キー I を求める；
3. 暗号化アルゴリズム E で連結されたIDが使用され、暗号化されたプログラム $X = E(P, I)$ を計算する；

暗号化解除のステップは以下のとおりである：

1. 予め形成されたID Bおよび固有のID Bを取得する；
2. 2つのIDが連結され（ $I = BU$ ）、暗号化／暗号化解除キー I を求める；
3. 暗号化解除アルゴリズム E^{-1} で連結されたIDが使用され、当初のプログラム $P = E^{-1}(X, I)$ を計算する；

図4を参照するに、本発明の第1実施例に関するブロック図が示される。マスタ・コンパクト・ディスクに関する周知のマスタ技術を利用して、プログラム可能なCD-ROMディスクがマスタされる（ステップ80）。この点に関し、例えば上述の共通して譲渡される米国特許出願番号09/662,561がある。プログラム可能なCD-ROMは第1セッション14を含むが、それに加えて他のマスタ・セッションを含むことも可能である。マスタ・ディスクに含まれるものは、予め形成されたID 22である。その後ステップ82において、マスタ・ディスクを利用して、標準的なスタンプ(stamp)手法によりプログラム可能なCD-ROMディスクを製造する。この時点では、多数の同一のプログラム可能なCD-ROMディスクが存在する。

【0030】その後ディスク10は各自の識別子を利用して書き込まれる。ステップ84において、固有のID 24が形成される。固有のID 24は、ディスク10の製造順によって定められるところの連続的に定められた番号とすることが可能であり、完全にランダムな番号とすることも可能であり、または予め形成された番号のテーブルから選択することも可能である。他の好適な実施例では、その番号はアルゴリズムによって更に処理され、そのアルゴリズムは、有効な番号(valid number)はとり得る番号の範囲内の小さな部分にのみ対応しているように使用番号(actual number)を生成可能である。この場合、有効な番号は、そのような生成アルゴリズムを知ることによってのみ作成可能である。また、この場合

は、検査アルゴリズムを提供し、例えば周知の公開キー、プライベート・キー暗号化および署名の手法を利用することによって、番号を認めることも可能である。他の実施例では、その番号はハードウェア身元確認により生成され、特定のコンピュータに関連付けられる。（この点については、例えばO' Connor et al., U.S. 5,745,568があり、本願でも使用可能である。）他の実施例では、固有のID 24が特定のアプリケーションに関連付けられ、このため同一の固有の識別番号が複数のディスク10上で使用される。固有のID 24は、書き込み済みセッションとなるISO9660両立可能ファイル・イメージを作成するために使用される（ステップ86）。このセッションの既知の絶対セクタ・アドレスに関する主チャネル・データは、固有のID 24を利用して修正され（ステップ88）、ステップ90において第2セッション16としてディスク10に加圧されずに書き込まれる。なお、このセッションは第3またはそれ以降のセッションとして書き込まれることも可能である。この時点において、各ディスク10は、各自自身の識別子を包含し、特有のものとなる。

【0031】顧客は暗号化に備えてディスク10を用意する。この段階は、ステップ74として図示され、図3で詳細に説明したセキュリティ・ソフトウェアによって実行される複数のステップより成る。固有のID 24は、第2セッション16における既知の絶対セクタ・アドレスから読み取られる（ステップ92）。暗号化は、ステップ76として図示され、図3で詳細に説明した多数のステップより成る。暗号化が完了すると、ディスク10上の第3セッション18にラップされた実行可能なものが書き込まれる（ステップ94）。

【0032】図5を参照するに、本発明の第2実施例のブロック図が示され、固有のID 24および暗号化された実行可能なもの40が同じセッションに書き込まれている。これは、図4で説明したものと同ジステップをいくつか含んでいるが、その順序が異なる。プログラム可能なCD-ROMディスクは、マスタ・コンパクト・ディスクに関して周知のマスタ技術を利用してマスタされる（ステップ80）。この点に関し、例えば上述の共通して譲渡される米国特許出願番号09/662,561がある。プログラム可能なCD-ROMは第1セッション14を含むが、さらに他のマスタ・セッションを含むことも可能である。ディスク10に含まれているものは予め形成されたID 22である。その後ステップ82において、マスタ・ディスクを利用して、標準的なスタンプ手法によりプログラム可能なCD-ROMディスクを製造する。この時点では、多数の同一のプログラム可能なCD-ROMディスクが存在する。

【0033】顧客は暗号化に備えてディスク10を用意する。この段階は、ステップ74として図示され、図3で詳細に説明したセキュリティ・ソフトウェアによって

(7) 002-304809 (P2002-304809A)

実行される複数のステップより成る。固有のID24がステップ84で形成される。固有のID24は完全にランダムな番号とすることが可能であり、予め形成された番号のテーブルから選択することも可能である。固有のID24は、書き込み済みセッションとなるISO9660両立可能ファイル・イメージを作成するために使用される(ステップ86)。このセッションの既知の絶対セクタ・アドレスに関する主チャネル・データは、固有のID24を利用して修正される(ステップ88)。ステップ74で読み込んだ予め形成されたID22と共に、固有のID24を利用して、暗号化を行う。暗号化は、ステップ76として図示され、図3で詳細に説明した多数のステップより成る。暗号化が完了すると、ディスク10上の第3セッション18にラップされた実行可能なものが書き込まれる。

【0034】図6を参照するに、本発明によるエンド・ユーザで実行するための方法が示される。まず、エンド・ユーザはディスク10をCD-ROM、CD-RまたはCD-RWドライブにディスク10を挿入する(ステップ100)。ディスク10上で実行可能なプログラムが自動的に走り出したりは選択される(ステップ102)。プログラムは先ず対ハッキング(anti-hacking)サブルーチン34を使用して、ハッキングまたはコピー・プロテクト対策を打ち破るために使用され得るカーネル・デバッグ・ソフトウェア(kernel-debugging software)の検査を行う(ステップ104)。そのようなプログラムが存在すると、そのプログラムはユーザにエラー・メッセージを示し、自動的に停止する(ステップ106)。

【0035】そのようなハッキング・ソフトウェアがエンド・ユーザのシステムに存在しない場合は、ステップ108において暗号化解除プログラムがドライブIDを読み出す。ステップ110において、暗号化解除プログラムは、そのドライブに対して、ATIP信号から予め形成されたID22を読み出すための命令を発行する。そして、ステップ116において、暗号化解除プログラムは、そのドライブに対して、第2の(後続の)セッションの主データ・チャネルの既知の絶対セクタ・アドレスから固有のID24を読み出すための命令を発行する。

【0036】ステップ118において、暗号化解除プログラムは、ステップ116で読み込んだ固有のID24と、ステップ110でATIPから読み込んだ予め形成されたID22とを連結する。ステップ120において、その連結された結果を暗号化解除キーとして利用して、ラップされたソフトウェア32の暗号化を解除する。ステップ122において、プログラムは、その暗号化解除が有効であるか否かを判定する。これを行ういくつかの手法が存在し、例えば、暗号化解除されたプログラム内のフラグを探索したり、オペレーティング・シス

テム固有のコードが暗号化解除された実行可能なものの中に存在するか否かを検査することが可能である。暗号化解除に失敗すると、エラー・メッセージが示され、そのプログラマーおよび全プロセッサが終了する(ステップ106)。暗号化解除が成功すると、当初の実行可能なものが開始される(ステップ124)。

【0037】暗号化解除プログラムは背景に残り(ステップ148)、プログラムは実行され(ステップ146)および抜け出す(ステップ150)。当初のプログラムが抜け出ると、暗号化解除プログラムは、メモリおよび当初プログラムの使用したハード・ドライブの領域をクリアし(ステップ152)、終了する(ステップ154)。

【0038】図7を参照するに、本発明が様々な不当な試みからどのようにして保護するかが示されている。例えば、不正な者が正当なプログラム可能なCD-ROMディスクのコピーを作成し、それには、使用許諾されているが各自から更に拡布することは認められていないソフトウェアを含んでいる場合がある。目下利用可能なディスク・ライターを利用しておよびソフトウェアを書き込んで、CD-Rディスクにコピーを行うことが可能である(ステップ160)。しかしながら、予め形成されたID11がディスク10のATIPに含まれており、これはコピーされ得ない。CD-Rディスク不正者は、ATIP信号に暗号化された予め形成されたID22を既に所有している、または予め形成されたID22を何ら所有していない。このような場合において、偽造のディスクによる実行可能なプログラム30の実行は、正しくない予め形成されたIDを形成し(ステップ162)、暗号化解除に失敗してしまう(ステップ164)。

【0039】また、不正者が1つ又はそれ以上の正当に登録されたプログラムを有するプログラム可能なCD-ROMディスクを有するが、他のユーザのプログラム可能なCD-ROMディスクから他のプログラムを不当にコピーする場合がある(ステップ166)。この分配が同一の分配者によるものである場合、ソースおよびターゲット・ディスクは同一の予め形成されたID22を有する。しかしながら、盗まれたプログラムは、それが配信元(originator)により正当に登録されているならば、予め形成されたID22および配信元の固有のIDの組み合わせによって暗号化される。不正者が盗んだプログラムを走らせようとする場合に、プログラムは、予め形成されたIDと不正者の固有のID(配信元の固有のIDとは異なる)とを利用して暗号化解除が行われる(ステップ168)。この手順は正しくないキーを形成し、ステップ164で暗号化に失敗する。

【0040】配信元から上記のプログラムを不当にコピーする際に、不正者が固有のID24の重要性に気付いており、そのコピーをも形成する場合がある(ステップ

(8) 002-304809 (P2002-304809A)

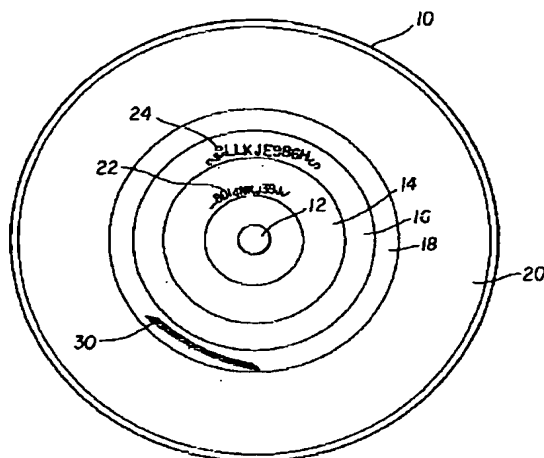
170)。固有のID 24は、ユーザの書き込み可能な領域内におけるディスク10の新たな部分に書き込まれる(ステップ172)。しかしながら、暗号化解除プログラム30は、ステップ116において、その固有のID 24が所定の場所にあることを期待している。したがって、暗号化解除プログラムは、ステップ168において不当な固有IDを利用して、配信元の固有のIDを利用して暗号化されているプログラムの暗号解除を試み、その暗号化解除に失敗する(ステップ164)。

【0041】不正者が固有のID 24だけでなく、所定の場所に位置する必要性にも気付いている場合もあり得る。その者は、ステップ170においてソフトウェアおよび固有のID 24をコピーする際に、配信元の固有のIDが、ディスク10上に既に位置している固有のID 24に上書きされるように、巧妙な制御を行うこともあり得る(ステップ174)。しかしながら、ディスク10への1文字の書き込みであっても、古い固有のID 24が消去されることは許容されず、利用できない新たな固有のIDを書き込んでしまう(ステップ176)。ディスク10におけるプログラムの更なる暗号化解除は失敗してしまう(ステップ164)。

【図面の簡単な説明】

【図1】図1は、本発明によるコピー・プロテクトを有するコンパクト・ディスクの平面図である。

【図1】



【図2】図2は、コピー不可能にアプリケーションを暗号化するソフトウェア手法の概略図である。

【図3】図3は、暗号化されたソフトウェアを形成するためのステップを示すブロック図である。

【図4】図4は、コピー・プロテクトがCDにどのように提供されるかの一例を示すブロック図である。

【図5】図5は、コピー・プロテクトがCDにどのように提供されるか他の例を示すブロック図である。

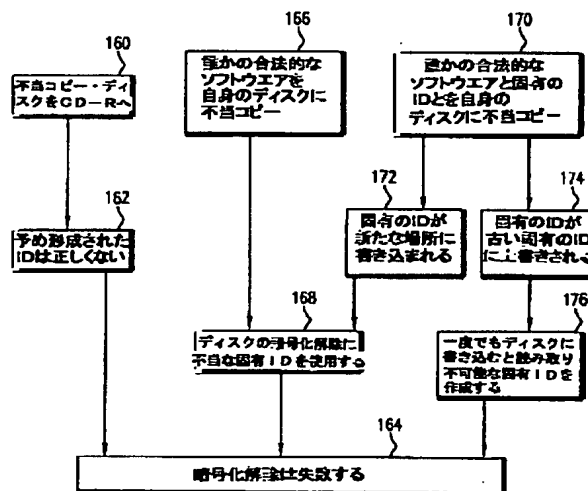
【図6】図6は、CDが読み込まれる場合に、コピー・プロテクトがどのように機能するかを示すブロック図である。

【図7】図7は、ここに開示したコピー・プロテクトが、それを破ろうとする方法をどのようにして阻止するかを示すブロック図である。

【符号の説明】

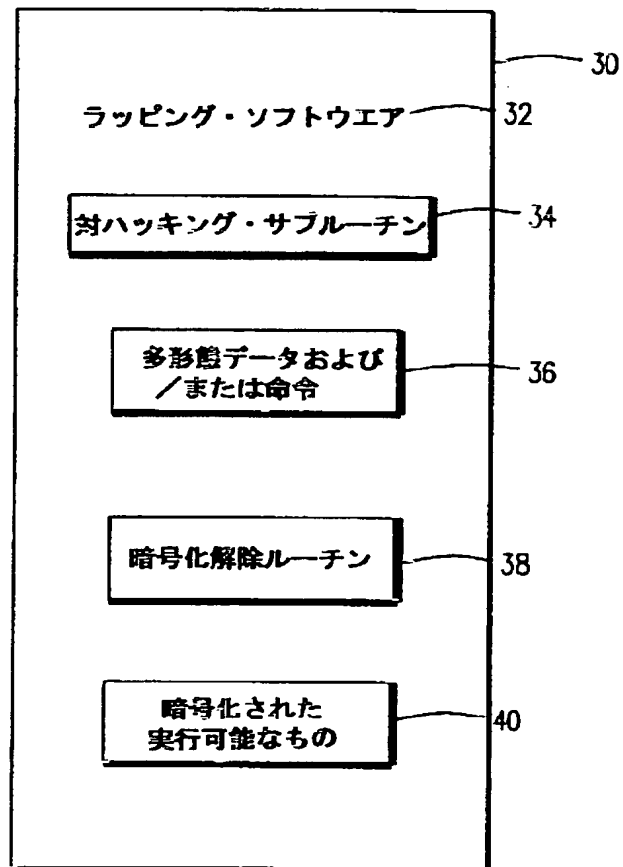
- 10 光学ディスク
- 14 第1セッション
- 16 第2セッション
- 18 第3セッション
- 20 再記録可能な領域
- 22 予め形成されたID
- 24 固有のID
- 30 パッケージ

【図7】



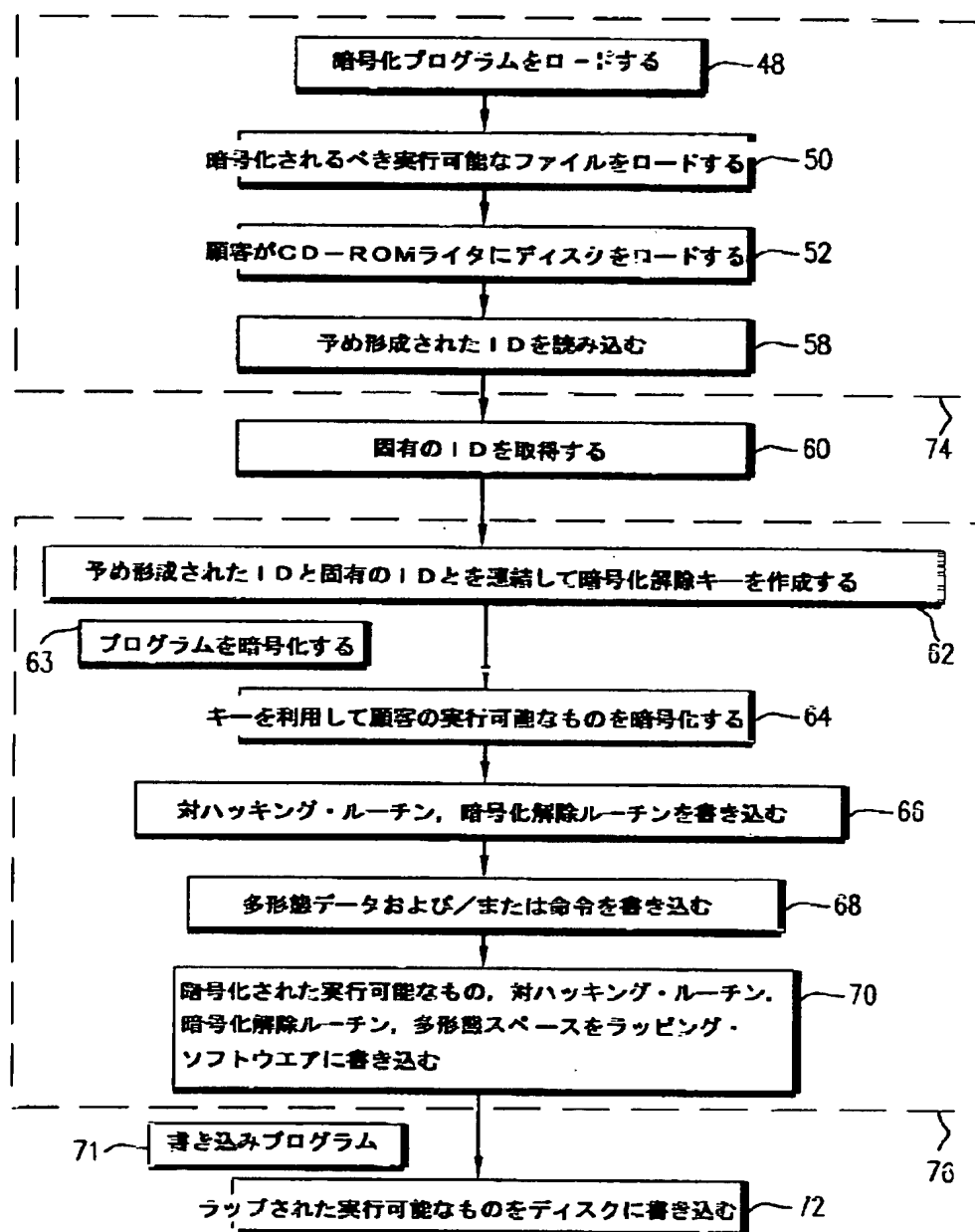
(9) 002-304809 (P2002-304809A)

【図2】



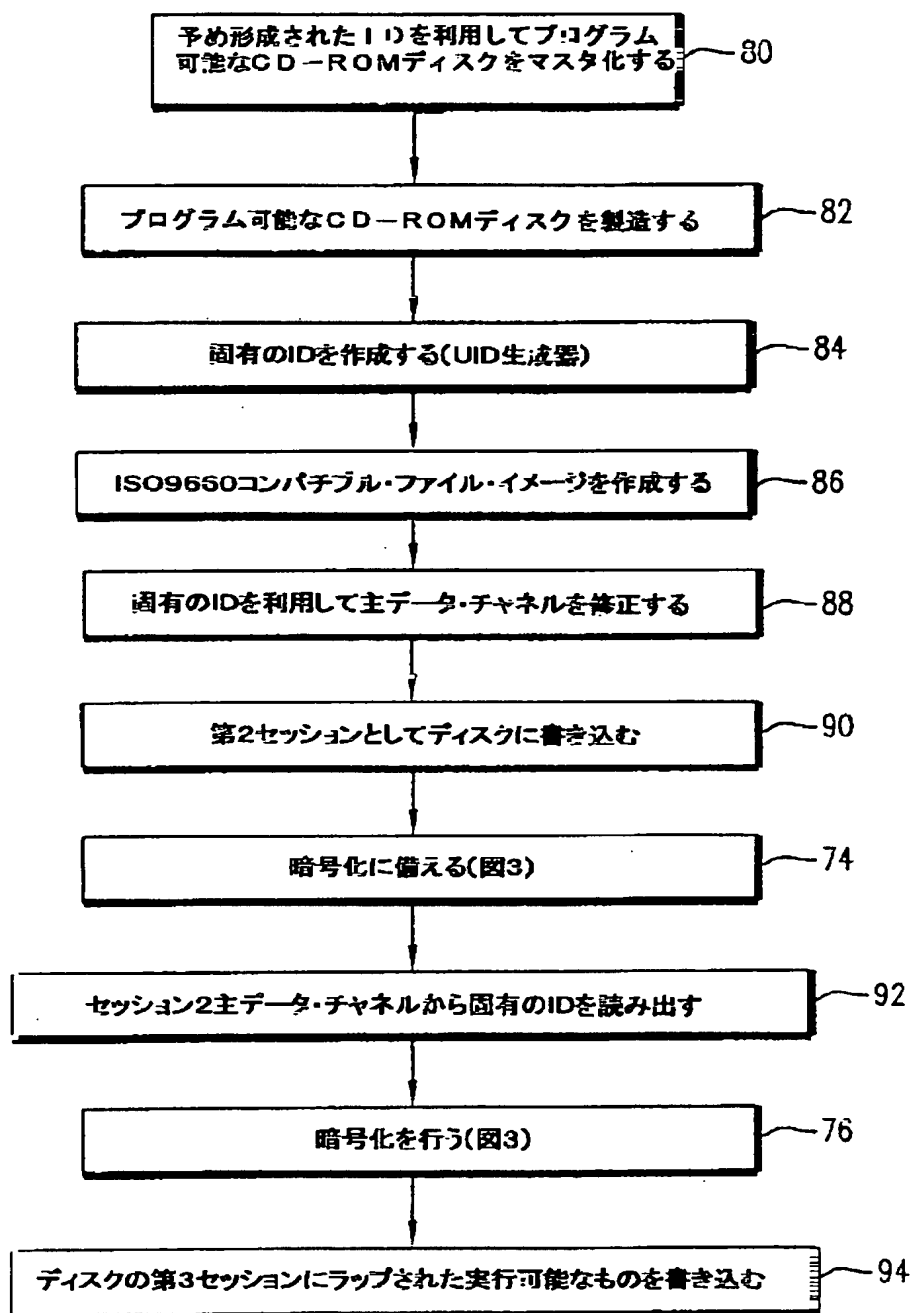
(株) 102-304809 (P2002-304809A)

【図3】



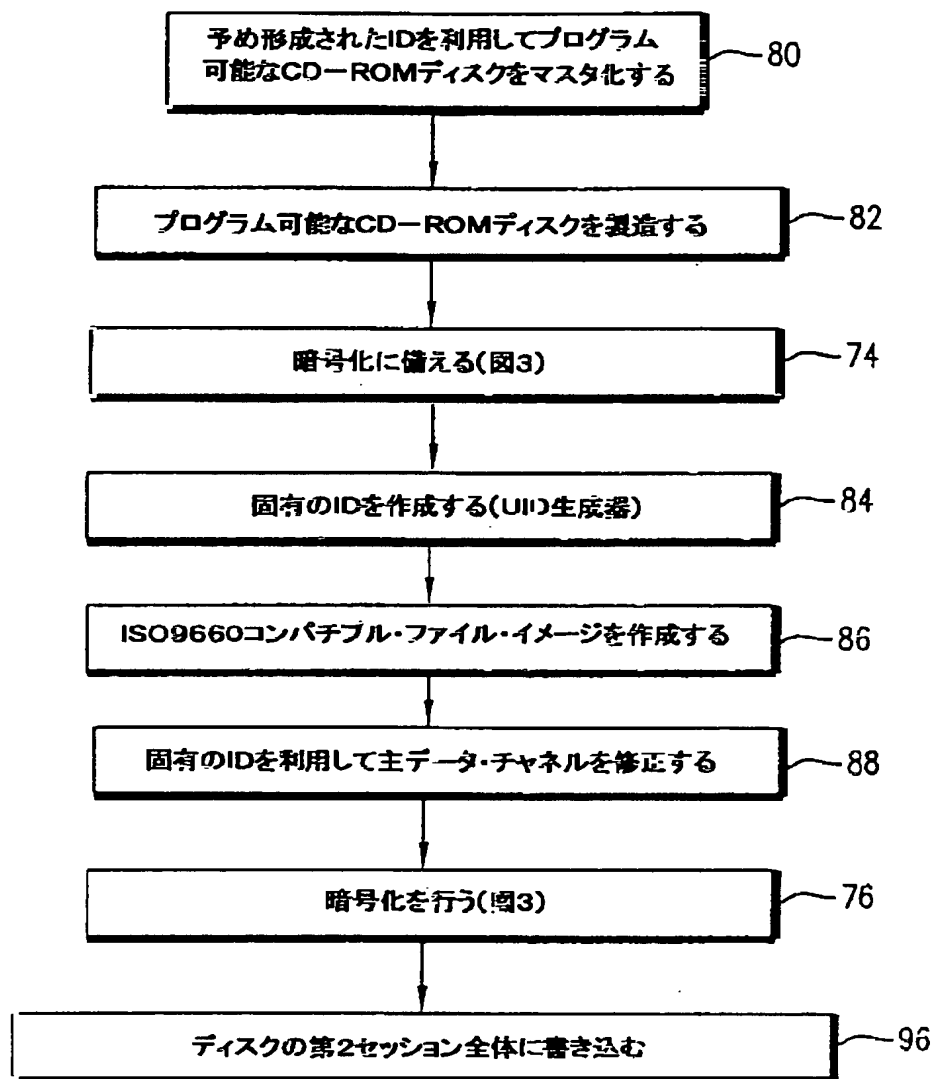
(特1) 02-304809 (P2002-304809A)

【図4】



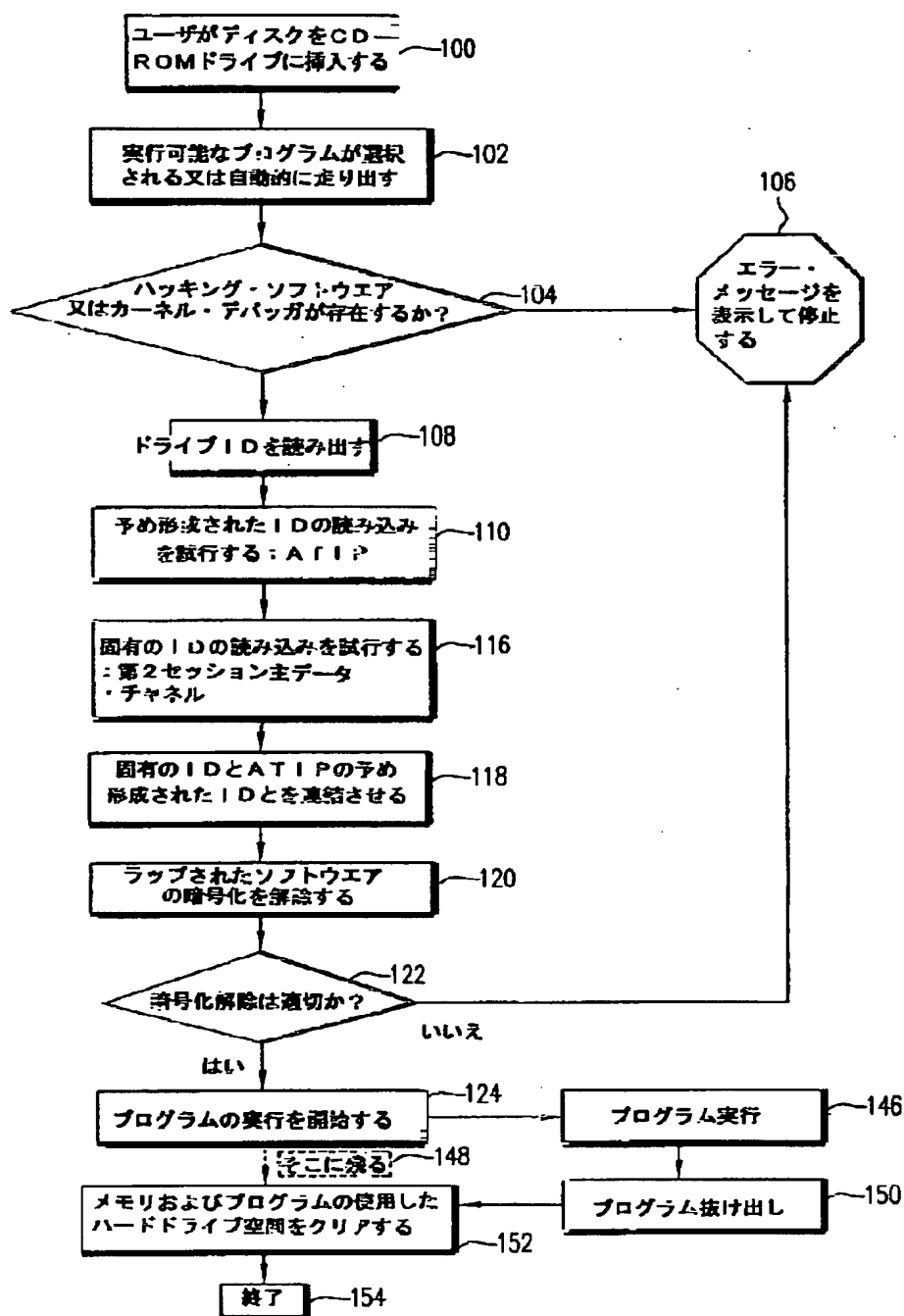
(株) 2002-304809 (P2002-304809A)

【図5】



(13) 102-304809 (P2002-304809A)

【図6】



フロントページの続き

(51) Int. Cl. 7

G 1 1 B 20/12

識別記号

F I

G 1 1 B 20/12

(参考)

(4) 1 0 2 - 3 0 4 8 0 9 (P 2 0 0 2 - 3 0 4 8 0 9 A)

(72)発明者 ブルース エル ハ
アメリカ合衆国 ニューヨーク 14580
ウェブスター レイク・ロード 1072

Fターム(参考) 5B017 AA06 AA07 BA07 CA09 CA15
5D044 BC03 CC04 DE49 GK17
5D090 AA01 BB02 CC12 FF09 GG32
HH01
5D121 JJ05 JJ08 JJ09